

UNITED STATES DISTRICT COURT

FILED

for the

JAN 28 2025

Northern District of Oklahoma

Heldi D. Campbell, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of)
 an Apple-brand Smartphone, Silver in Color with no External)
 Markings and is Contained in a Clear Case, Currently Stored at)
 the Broken Arrow Police Department Digital Forensic Lab at)
 1101 North 6th Street, Broken Arrow, Oklahoma)

Case No.

45-MJ-64-JFJ

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 875(c)

Interstate Communication

18 U.S.C. § 35(b)

Imparting or Conveying False Information

The application is based on these facts:

See Affidavit of Brian Deliberato, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Brian Deliberato

Applicant's signature

SA Brian Deliberato, FBI

Printed name and title

Subscribed and sworn to by phone.

Date:

1/28/25

Jodi Jayne

Judge's signature

City and state: Tulsa, Oklahoma

Jodi F. Jayne, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of an
Apple-brand Smartphone, Silver in
Color with no External Markings and
is Contained in a Clear Case,
Currently Stored at the Broken Arrow
Police Department Digital Forensic
Lab at 1101 North 6th Street, Broken
Arrow, Oklahoma**

Case No. _____

FILED UNDER SEAL

**Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize**

I, Special Agent Brian Deliberato, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I am a Special Agent with the Federal Bureau of Investigation assigned to the Oklahoma Joint Terrorism

Task Force based in Tulsa, Oklahoma. As a Special Agent, my duties include investigating violations of federal criminal law and threats to national security. In addition to formalized training, I have received extensive training through my involvement in an array of investigations working alongside experienced law enforcement officers at both the federal and local level. My investigations include, but are not limited to, violent crimes, counterterrorism, and cybercrimes.

3. Specifically, I have experience working investigations which commonly include violations of 18 U.S.C. §§ 875(c) and 35(b), respectively.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 875(c) (Interstate Communication) and 18 U.S.C. §§ 35(b) (Imparting or Conveying False Information) will be located in the electronically stored information described in Attachment B and is recorded on the device described in Attachment A.

6. 18 U.S.C. § 875(c) states in relevant part:

Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

7. 18 U.S.C. § 35(b) states in relevant part:

Whoever willfully and maliciously, or with reckless disregard for the safety of human life, imparts or conveys or causes to be imparted or conveyed false information, knowing the information to be false, concerning an attempted or alleged attempt being made or to be made, to do any act which would be a crime prohibited by this chapter or chapter 97 or chapter 111 of this title shall be fined under this title, or imprisoned not more than five years, or both.

Identification of the Device to be Examined

8. The property to be searched is an Apple-brand smartphone, silver in color with no external markings and is contained in a clear case hereinafter the “Device.” The Device is currently located at the Broken Arrow Police Department in the digital forensic lab at 1101 North 6th Street in the City of Broken Arrow, Oklahoma.

9. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

Probable Cause

10. In December 2024, FBI Oklahoma City was made aware of an individual with the name Rockstar Jericho Burright for making threatening telephone calls to the Empire State building, located in New York City, New York, to include threats regarding the use of explosives. Burright was identified in police reports as a fifteen-

year-old juvenile. The telephone calls occurred on November 19, 2024, and November 20, 2024. The telephone calls were made using electronic communication that were transmitted through interstate communications.

11. On December 20, 2024, FBI Oklahoma City requested and received verification from the Muscogee (Creek) Nation Citizenship Office that Rockstar Jericho Burright is enrolled with the Muscogee (Creek) Nation and has been since September 27, 2017.

12. The following information was provided to FBI Oklahoma City by the Broken Arrow Police Department, the information is regarding New York Police Department (NYPD) Case Number LIU-2024-1020-C:

- a. “On Sunday, November 17, 2024, at approximately 1415 hours, the IDOU¹ was notified by Philip Passante, Empire State Building security, via NYC Safe Hotline in regard to a bomb threat to the Empire State Building located at 350 5th Avenue within the confines of Midtown North.”
- b. “On Sunday, November 17, 2024, at approximately 1406 hours, an unknown male called multiple times to the Empire State Building observatory, stating he wanted to aggressively bomb the building, and he placed C4² on top of the building. He also stated in 34 minutes it’s

¹ Based on a review of the New York Police Department reports provided to the FBI, by the Broken Arrow Police Department, “IDOU” is referring to Sgt. Toal of the New York Police Department.

² According to open-source research “C4” is most likely referring to a type of plastic explosive.

on. Empire state building security and K9 canvassed the perimeter of the building and the observatory and found nothing suspicious. MTS³ responded to location and canvassed building with negative results.”

- c. “Location: Empire State Building 350 5th Avenue, New York, NY 1001”
- d. “POI⁴: 918-703-2420 and 918-553-3907”
- e. “On Sunday, November 17, 2024, the I/O⁵ conducted a phone interview with Philip Passante (Empire State Building) regarding a bomb threat to the empire state building. Mr. Passante informed the I/O that they received two calls from two separate number stating that a bomb is placed inside of the building.” ... The I/O also inquired about both phone numbers that made the threat if they had any previously calls. Mr Passante responded no.”

13. The following information was provided to FBI Oklahoma City by the Broken Arrow Police Department, the information is regarding Broken Arrow Police Department Case Number 2024-08670:

- a. On November 19, 2024, Detective Graham with the New York Police Department provided the following information to the Broken Arrow Police Department, “the NYPD had identified the telephone number

³ Based on open source research “MTS” stands for “Midtown South”. In this specific use of MTS it is referring to the New York City Police Department’s Midtown South Police Precinct.

⁴ “POI” commonly refers to Person of Interest

⁵ “I/O” commonly refers to Investigating Officer

associated with the bomb threat and that an analyst had identified a suspected caller. The number 918-703-2420 belonged to Miranda Burright, 1828 N. 15th Street Broken Arrow, OK in Tulsa County. The NYPD believed Rockstar Jericho Burright made the threats to the Empire State Building”.

14. The following information was provided to FBI Oklahoma City by the Broken Arrow Police Department, the information was provided to the Broken Arrow Police Department by NYPD Detective Graham:

- a. “We just received another bomb threat from the phone number 918-703-2420”.
- b. “On Wednesday, November 20, 2024, at approximately 2114 hours, the IDOU was notified by P.O Suh from MTS Pct. Via NYC Safe Hotline in regard to a bomb threat to the Empire State Building located at 350 5th Avenue, New York, NY 10118, within the confines of Midtown South.”
- c. “On Wednesday, November 20, 2024, at approximately 2040 hours, an unknown male called Will Call at the Empire State Building, stating a bomb was going to go off at the Empire State Building in 15 minutes. Empire state building security and K9 canvassed the perimeter of the building and the observatory and found nothing suspicious. MTS responded to the location and canvassed the building with negative results.”

d. "POI: Unknown Male 918-703-2420"

e. "Location: Empire State Building 350 5th Avenue New York, NY
10118"

15. The following information was provided to FBI Oklahoma City by the Broken Arrow Police Department, the information is regarding Broken Arrow Police Department Case Number 2024-08670:

a. On November 21, 2024, Detective Williamson with the Broken Arrow Police Department called 918-553-3907. The following information was provided in the police report regarding the telephone call; "A male voice answered the telephone. I identified myself and asked who I was speaking with, and the voice stated this was Rockstar."

16. On November 21, 2024, Detective Williamson and Detective Gilbert with the Broken Arrow Police Department conducted a voluntary and consensual interview at Burright's residence located at 1828 N. 15th Street, Broken Arrow, Oklahoma. The interview location was within the established boundaries of the Muscogee Creek Nation. Also present for the interview was Rockstar Burright and his parents. The following information regarding the interview was provided to FBI Oklahoma City by the Broken Arrow Police Department, the information is regarding Broken Arrow Police Department Case Number 2024-08670:

a. "Rockstar admitted to making the bomb threat phone calls to the Empire State Building."

- b. “Rockstar stated he was with another friend, who suggested he call the Empire State Building and make the bomb threat. When asked who his friend was, Rockstar stated he would not ‘snitch’ and refused to give the friend’s name.”
- c. “I asked Rockstar where his phone was, and Rockstar patted his right pant pocket, indicating that the phone was there.”
- d. “Rockstar identified the phone numbers as his phone numbers. The number 918-703-2420, which is registered to Rockstar’s mother, is the phone number for his phone, an Apple iPhone. Additionally, Rockstar identified 918-553-3907 as his “fake” phone number.”
- e. “Rockstar had removed the phone he used to make the bomb threats to the Empire State Building from his pocket, and it was in his hand, in plain view. I seized the phone from his hand and informed him I was seizing the phone as evidence.”

17. The Device is currently in the lawful possession of the Broken Arrow Police Department. It came into the Broken Arrow Police Department’s possession in the following way: Based on information provided to the FBI by the Broken Arrow Police Department Case File 2024-08670 the device was in plain view and was seized as evidence of a crime.

18. The Device is currently in storage at the Broken Arrow Police Department’s Digital Lab located at 1101 North 6th Street, Broken Arrow, Oklahoma.

19. Your affiant requests a search warrant for the device. According to the interview of Burright, he is the owner and operator of the telephone numbers 918-703-2420 and 918-553-3907. According to the interview of Burright, he used the device to contact the Empire State Building and falsely convey threatening communication on November 17, 2024.

20. Your affiant believes the requested search of the device, for the items contained in Attachment B, may contain evidence of violations of 18 U.S.C. § 875(c) (Interstate Communication) and 18 U.S.C. §§ 35(b) (Imparting or Conveying False Information). Specifically, the device may provide additional information regarding Burright's research in reference to infrastructure of high importance or profile to include contact information. Communications with other individuals referencing the threatening communication or plans to commit additional acts of transmitting threatening communication. Further, the device may provide evidence whether Burright has conducted research and/ or attempted to or successfully obtained material to construct an explosive device such as the ones that were referenced in the telephone calls to the Empire State Building November 19, 2024, and November 20, 2024.

Technical Terms

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data

communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This

storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using

specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated

by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

22. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

Electronic Storage and Forensic Analysis

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have

been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities, including providing material support or resources to designated foreign terrorist organizations or other co-conspirators. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

25. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like "Instagram", "Facebook", "Telegram", "Whatsapp", and "GroupMe." Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted

at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual. This data includes contacts used to conduct illegal activities to include providing material support or resources to designated foreign terrorist organizations and fraud and related activity in connection with access devices.

26. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the cellular telephone.

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted

portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to unauthorized access to a victim’s electronic access device over the Internet and providing

material support or resources to designated foreign terrorist organizations the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

19. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

20. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

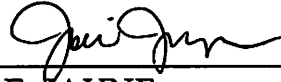
21. I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

Brian Deliberato

Brian Deliberato
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to by phone on January 28th, 2025.



JODI F. JAYNE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The property to be searched Apple-brand smartphone, silver in color with no external markings and is contained in a clear case hereinafter the “Device.” The Device is currently located at the Broken Arrow Police Department in the digital forensic lab at 1101 North 6th Street in the City of Broken Arrow, Oklahoma.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records on the Device(s) described in Attachment A that relate to violations of 18 U.S.C. § 875(c) (Interstate Communication) and 18 U.S.C. §§ 35(b) (Imparting or Conveying False Information) including:

1. Records relating to communication with others as to the criminal offense(s) listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
2. Records relating to documentation or memorialization of the criminal offense(s) listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;
3. Records relating to the planning and execution of the criminal offense(s) above, including Internet activity, firewall logs, caches, browser history, and cookies, “bookmarked” or “favorite” web pages, search terms that the user

entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;

4. Application data relating to the criminal offense(s) listed above;
5. Threatening communications related to the criminal offense(s) listed above;
6. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;
7. All records and information related to the geolocation of the Device and travel in furtherance of the criminal offense(s) listed above; and
8. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the criminal statutes listed above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, and instrumentalities described in this warrant. The review of this electronic data

may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.